Uppsala University

Department of Informatics and Media

Big Data Infrastructure for Cloud Computing

Author

Hafiz Muhammad Qasim Amin

Super Visor

Franck Tétarad

Abstract

It is becoming increasingly common for "cloud" organizations to provide information technology services and for businesses and individuals alike to use information technology resources in new ways due to cloud computing. Cloud computing security issues and software failures are examined in the literature survey. Papers were examined for the review using a modified version of the procedure Okoli and Schabram (2010) described, but only 12 were included in the final output. Even though numerous security flaws and solutions have been discovered, it has become evident that much of the current research is just theoretical. As a result of this analysis, future research should pay more attention to these security issues.

Keywords

Software failures, security issues, cloud computing, systematic literature review

Table of Contents

List of Figures

List of Tables

Abbreviation

AI	Artificial Intelligence
ANSI	American National Standards Institute
AES	Unauthorized Access
CSPs	Cloud Service Providers
DAS	Direct-attached storage
DSE	Data Encryption Standard
EDA	Event-Driven Architecture
FT	Fault Tolerance
IaaS	Infrastructure as a Service
IoT	Internet of Things
I/O	Input/output
IT	Information Technology
LAN	Local Area Network
NAS	Network-Attached Storage
PaaS	Platform as a Service
RSA	Rivest-Shamir-Adleman encryption
SLR	Systematic literature Review
SaaS	Software as a Service
SAN	Storage Area Networks
SLA	Service Level Agreement
VM	Virtual Machine

Preface

A large-scale cloud platform uses Big Data and cloud computing. The cloud data service may store data in parallel, allowing for data sharing simultaneously. In this scenario, the service provider must maintain data integrity, privacy, and confidentiality. The storing, retrieving, and sharing of data are the primary causes of concerns regarding cloud computing security. As the load-balancing continues, reliability problems cause the software to malfunction. Therefore, software failure and security concerns are the two most significant problems associated with cloud computing. Researchers have proposed several frameworks, strategies, and models to solve software vulnerabilities. We focus on reviewing papers from 2019 to 2022 to identify major security issues and software failures during these years.

1 Introduction

The most critical cloud computing threats are data security and privacy. The main concern for the organization is to provide safety of necessary data between the cloud and their data center and when it is stored and processed at a third-party data center. Because of characteristics such as authorization and legal access, it is possible to employ additional resources in the cloud, although secure computation can be challenging. Other security threats include privacy, integrity, secrecy, and the availability of stored data.

1.1 The architecture of Cloud Computing

Computing on the cloud is currently one of the most discussed and widely used technologies. It gives any firm a modern look by providing them with virtualized services and resources that can be accessed whenever needed. Regardless of its size, every small, medium, or large company uses cloud computing services to store information and access that information via the Internet from any location—a deeper understanding of the inner workings of cloud computing and how it operates.

Every cloud design should include the most important restrictions, including openness, scalability, security, and intelligent monitoring. The current study on other key limits assists the development of new features and strategies for the cloud computing system (Ali & Gregory, 2020).

1.1.1 Cloud Computing Architecture

The cloud architecture is distributed into two portions

i. Frontend

ii. Backend

Cloud computing design uses (Service-Oriented Architecture) SOA and EDA, which stands for enterprise data architecture (Event-Driven Architecture). The customer infrastructure, the application, the service, the runtime, the storage, the infrastructure, the organization, and the security are all known as the cloud computing architecture (Odun-Ayo & Agono, 2018)

1. Frontend

In the cloud computing system, the front end refers to the client-side. In other words, it includes all the client-side tools needed to access the cloud computing services/resources provided by the cloud computing service provider. Use a web browser, for example, to gain access to a cloud computing platform.

- **Client Infrastructure –** Client Infrastructure is a name for the front-end pieces. It has the user interfaces and applications needed to access cloud computing.

Complex computations can be done on a huge scale using cloud computing. Maintaining expensive computer hardware, software, and space is no longer necessary. The concept of cloud computing is well-known. Because of the time and resources required, handling massive data requires a well-developed computing infrastructure.

As a result of the proliferation of social media, the Internet of Things, and multimedia platforms, businesses are collecting an ever-increasing quantity of data. Because of this, there is a vast amount of structured and unstructured data. This phenomenon is referred to as "big data," and it is rapidly developing into a trend in the industry. "Big data" concept is rapidly gaining traction in academia, government, and the commercial industry. Big data is distinguished by its vast volume, the impossibility of storing it in standard relational databases, and the speed it generates, collects, and analyses. These three features come together to form the definition of big data. Big data affects not just the field of medicine but also engineering and the financial industry.

2. Backend

We will refer to the service provider's cloud when discussing the backend. It stores the resources, ensures that they are in good condition, and provides protection to secure those resources. In addition, it consists of a considerable quantity of storage, virtual applications and computers, traffic control systems, and deployment models, among other things.

Application – Any software or platform customers have access to is an application in the backend. As a result, the service is tailored to the customer's needs.

1. **Cloud Runtime** provides a platform for the virtual machine's execution and runtime environment called "backend cloud."
2. **Infrastructure –** In the backend, cloud infrastructure refers to the servers, storage, network devices, virtualization software, and other cloud-like hardware and software failure.
3. **Storage –** Backend storage refers to the flexibly and scalable management of stored data.
4. **Management –** Application, storage, runtime cloud, Infrastructure, and other security measures are examples of backend faults that can be managed.

5. **Internet –** An Internet connection is required to establish interaction and communication between the frontend and backend.
6. SaaS, PaaS, and IaaS are the most common cloud-based service models. It also controls the service type the user can access at any time.
7. **Security –** For cloud resources, systems, data, and infrastructure, security in the backend means implementing various security techniques.

The different types of data organizations store demonstrate how advancements in data storage and mining have made it possible to monitor an increasing amount of information. Cloud computing systems are required for data analysis and applications that demand frequent updates. These systems may evolve faster than academics and industry professionals. The utilization of cloud computing is one of the furthermost significant originations in current information technology and business applications. It has developed into a powerful instrument that can perform complex computing on a huge scale. Cloud computing offers a variety of benefits, including the utilization of virtualized resources, parallel processing, and increased levels of safety. With the support of cloud computing, computer automation can be accomplished with less effort and at a lower cost. In addition, it can reduce the cost of maintaining the infrastructure, simplify management, and broaden the range of access options available to customers. Many cloud-based applications have been developed due to these numerous benefits. Because of this, the amount of data these applications produce and use has greatly expanded over the pastfew years.

Some initial users of cloud-based Big data solutions, such as IBM Bluemix, Microsoft Azure, and then Amazon AWS. Cloud computing can be created using various technologies, including virtualization, one of those technologies. In the context of big data or cloud computing, virtualization serves as the basis for various platform functionalities. These functionalities are essential for accessing, storing, analyzing, and managing various distributed computing methods. Sharing resources while completely isolating the hardware is a practice known as virtualization. This technique aims to make computers more effective, useful, and scalable. Investigating the current state of big information stored in cloud computing schemes is the primary research topic in this field.

1.2 Cloud computing and Big Data

Cloud computing and big data enables operators to comportment distributed queries over numerous datasets and swiftly deliver result sets using standard computing techniques. Cloud computing relies on Hadoop, a platform that allows for data processing dispersed across multiple computers. Instead of using local storage connected to a processor or another device, information is stored using a technology known as distributed storage created on cloud computing. The evaluation of big data is powered by cloud-based presentations, which are expanding rapidly and are constructed using virtualization technologies. Therefore, calculating in the cloud is not only a method for computing and processing vast amounts of data but also a method for running a business.

1.3 Cloud security

As one of the utmost promising and challenging computer expertise, cloud security offers users a wide range of communication options. As with cloud data security, a new trend in data innovation necessitates an increase in security. Data centers are familiar places where information is stored and managed but not impassable. Many various types of attacks have the potential to damage them. As a result, there must be a safe and secure means to alter data on servers while preserving customer privacy. Such information is sent and kept in the cloud server using the various services. A variety of encryption methods protected the cloud's data.

1.4 Cloud computing characteristics

A cloud computing system has various services that use resources in various ways, and dynamic application resource requirements frequently alter. Cloud computing systems must ensure that dynamically offered resources are dependable and do not interfere with the efficient use of resources, although service systems fail. All methods of enhancing dependability have identical drawbacks. Large-scale cloud computing systems cannot gather accurate error data because of their size and complexity. In some cloud computing setups, data created at random is employed. Natural cloud computing infrastructures cannot easily demonstrate their reliability or utilize optimization approaches (Bello & Oyedele, 2021).

Computing in the cloud is seeing rapid growth and has already established itself as a fixture in the next compeers of information technology companies and organizations. Cloud computing offers dependable IaaS, software, and hardware services with the Internet of Things (IoT). It is now feasible to carry out intricate and extensive computer tasks on a wide scale using cloud services. These services encompass a broad range of information technology duties, ranging from storing and calculation to database and application services, among other things. Cloud computing is becoming increasingly popular among individuals and corporations as a solution to the challenges of storing, managing, and analyzing massive quantities.

1.5 Service-Oriented Architecture (SOA) impact on the organization

Managing and utilizing hardware and software resources in a cloud-based system is critical. Because of the Service-Oriented Architecture (SOA) that underpins cloud computing, businesses can share their physical and non-physical IT infrastructures. The goal of reusing computing infrastructure as many times as possible is to spread out computing costs. Aside from the decreased initial investment and operating costs, these qualities have many other advantages. There are a variety of ways in which cloud computing affects various people. Shared information and communication technology can help e-commerce workers (Bello & Oyedele, 2021). Along with these models and deployment methods, this framework also incorporates three more categories of services: platform-as-a-service (PaaS), software-as-a-service (saas), and infrastructure as a service (public, private, community, and hybrid).

1.6 Aspects of cloud computing

Due to the distributed nature of their systems, cloud services can be retrieved from any internet-connected device. Multiple persons and apps may use the infrastructure because of the shared pool functionality. Thus, the same computer infrastructure can be used by many people without being concerned about their privacy or security. The elasticity feature makes the ease of adjustment of computer resources possible. A company that suddenly sees new clients can rapidly expand its cloud infrastructure to accommodate them (Bello & Oyedele, 2021).

On the other hand, "on-demand self-service" refers to customers not having to request computing services. Before the advent of cloud computing, customers had to order computers, wait for them to arrive, and set up their devices. It takes hours to come back up and running. There is no need for computer users to go to the cloud provider's website and provide their credit card information; they may immediately begin using the computer resources. Cloud consumers may self-manage their services and only pay for what they use using the web service portal, saving them money on unnecessary services. Cloud resources are likewise tallied in the same way energy and water are metered. At the end of the month, users receive a bill for the amount they used, and they pay that amount.

1.7 Cloud computing models

There are three cloud service models, from virtual hardware to application-specific users. The technological layer, also known as infrastructure-as-a-service, provides users with remote access to storage and servers that may be used for data analysis. Customers can increase or decrease the size of their virtual storage space as needed, which they can do via the Internet. However, cloud storage is simple and costs a fraction of a traditional hard drive. It's also very safe to use this method. The application layer, or platform-as-a-service, allows developers to construct apps. Data from many on-site and back offices can be combined via a PaaS. As a result, ownership costs are cheaper. These are just a few SaaS(software as a service) services commonly used in the construction industry (Bello & Oyedele, 2021).

Many applications for large-scale experimentations are being organized on the cloud, and it is projected that this number will continue to grow as computing resources in local servers become scarcer and capital prices decline. The volume of information produced by and disbursed by tests continues to expand. Users can admit cloud resources and install their applications if cloud service providers integrate parallel data processing frameworks into their offers. According to the definition found on Wikipedia, the core concept behind cloud computing is the ability to gain on-demand network contact to a variety of pre-configured calculating resources, which can be hastily provisioned and released with the minimal determination required from management or interaction with service providers. The usage of cloud computing offers some benefits, including the quicker growth of economies and reducing technological impediments. As a result of cloud computing, organizations may concentrate on their essential operations without being bothered by peripheral problems such as organization, adaptability, and the obtainability of resources. Due to the utility model of cloud computing and the enormous amount of calculations, infrastructures, and stowage cloud services currently available, researchers can carry out their tests in a highly desirable setting and favorable to their work. The most prevalent service models in the cloud are PaaS, SaaS, and IaaS.

1.8 Examples of cloud-based business models

It is possible to set up cloud services, including public, private, communal, and hybrid. Deployment models differ depending on how and who can utilize the service and how they can access it. Clients connect to the cloud service over the Internet when using a public cloud. One customer's data is handled alongside data from other customers in a multi-tenant system. Public cloud applications might be housed in a single data center or distributed. The cloud service provider is responsible for maintaining and administering the entire IT stack. For most small enterprises, the public cloud is the best option. Only one organization can use a private cloud. A cloud infrastructure hosted on-site. The only way to get to it is via the corporate intranet. The ideal option to keep sensitive data on a specialized system, such as national infrastructure, is private. Large corporations and government agencies should use this strategy to store sensitive data. Some organizations share cloud infrastructure in a community cloud model. Only participating organizations will be able to access the community cloud. Many deployment types can coexist in a hybrid cloud deployment in the same environment. Private clouds can be used for financial reporting, whereas public clouds can be used for telematics and other non-sensitive data.

1.9 Problem Area

A large-scale cloud platform uses big data and cloud computing. Data and schemes develop in quantity and complexity, data management, sharing, privacy, software failures, and security issues will occur. Cloud data services allow these issues to be resolved slowly, improving cloud computing speed. The cloud data service may store data in parallel, allowing for data sharing simultaneously. In this scenario, the service provider must maintain data integrity, data privacy, and data confidentiality (Mishra & Janarathanan, 2021), (Rady & Abdelkader, 2019). The storing, retrieving, and sharing of data are the primary causes of concerns regarding cloud computing. Many researchers have proposed several frameworks, strategies, and models to solve software vulnerabilities. The study has to examine thoroughly. In the end, a framework and recommendations for existing studies are required.

2 Background / Context

There are key services of cloud computing that provide the functionality to operate accurately on every client end. Thus, all the software failures and security issues concern these services. Some limitations of its services need to be considered while discussing software failure and security issues.

The rapid expansion of cloud computing platforms in size and computing capacity has resulted in significant issues with system management and upkeep: It is getting harder and harder to detect malfunctions in hardware and software. When an operation can manage failures, continual reliability planning is required. Large-scale cloud systems must be planned and implemented to provide high system dependability, operational flexibility, and automatic failure recovery as part of this strategy (regardless of location). More and more people have become accustomed to storing their commercial and organizational data in the cloud Operational and service excellence, strong security, long-term survival strategy, and competitive advantage are some of the business goals required by cloud computing. From the automation of manual labor to the fundamental shifts in business models made possible by the Internet, much technological advancement has led to enterprises' digital transformation. There is a need to create such a framework to handle software failures and security issues.

The main areas where the model developed are big data analytics, cloud computing, mobile technology, and application program interfaces (API).

There is a need to establish such a model that includes the characteristics of big data, a cloud computing platform for knowledge, relationships, and Big Data in the first phase, referred to as the "Big Data Enterprise." Analytics are then discussed as a way for firms to improve their results. Three main services of cloud computing facilitate the cloud to stream its services. These are Saas, IaaS and Paas. The data security must be maintained at the software level as a server. Each service requires maintained frequently to reduce the chance of failure and increase data security and privacy. Similarly, at PaaS and IaaS, data need to be protected. All the services have been discussed below with their main limitation.

On the other hand, there is a need for a unified infrastructure that can handle and analyze a wide range of service-generated big data. This is because the amount of data collected is always increasing. This work presents an overview of big data and Big Data As A Service. Big data generated by services can improve the system performance in several ways. As a result, to increase productivity and reduce costs, organizations are turning to Big Data as a Service (also known as infrastructure as a service, platform as a service, or software as a service) to provide common big data services (like access to service-generated big data and data analytics results). This is all included in Big Data as a Service.

2.1 SaaS: Software as a Service

Business owners who want to use the cloud prefer SaaS (Software as a Service, often recognized as "cloud application services"). SaaS allows customers to access apps hosted by a third party through the Internet. Business owners do not need to download or install anything on their computers to use most SaaS programs (Sultan & Ghani, 2019).

Data security. SaaS application's backend data centers may have to deal with large amounts of data to perform the essential software functions. A SaaS solution hosted in the public cloud may compromise security and agreement and considerable costs for moving massive data workloads if sensitive company information is transferred.

Lack of integration sustenance. Many enterprises require deep amalgamations with on-premise software, information, and services. Organizations may be forced to use internal resources to create and manage integrations if the SaaS vendor only provides minimal support. The more complicated the integrations, the less useful the SaaS app or other reliant services.

Interoperability. If the SaaS app is not built to be integrated with other apps and services, this can be a serious issue. SaaS services may not always be viable for organizations that need to create or streamline their integration systems.

Vendor lock-in. Signing up for a service may be made simple by the vendor, yet leaving the service may be difficult. For specimen, the information might not be theoretically or economically convertible between SaaS apps from different providers short of incurring a significant expense or requiring in-house engineering rework. This could be the case for some reasons. Every service provider does not utilize standard application programming interface protocols and tools, yet, the structures may be relevant to certain business activities.

Customization. SaaS apps allow for very little personalization. Without a universal solution, consumers may be constrained by the vendor's capabilities, performance, and other integrations. The wide range of customization is an advantage of using on-premises software development kits (SDKs).

Feature limitations. Organizations that want additional features from SaaS programs may have to forgo things like security, cost, performance, and other business standards. Moving suppliers or services to satisfy new feature demands may be impossible because of vendor lock-in, pricing considerations, or security concerns. These factors could make switching impossible.

Because the purveyor monitors the SaaS service, the provider's responsibility is to maintain the service's performance and security. Even with appropriate service level agreements (SLAs) in place to protect against unplanned and planned maintenance, cyberattacks, and network outages, the performance of the SaaS app may still be negatively impacted.

Lack of control. When utilizing SaaS solutions, it is necessary to relinquish some control to a third-party service provider. These limitations apply to the program and its data and governance (in terms of version, upgrades, and appearance). Because of the features and functionality offered by the SaaS service, users may need to reevaluate existing approaches to data protection and governance.

2.2 PaaS: Platform as a Service

More typical usage of the term indicates the supply of cloud platform services rather than cloud computing. PaaS provides a framework to build their own when it comes to app development. The organization or a third-party provider can handle servers, storage, and networking, but the apps will remain in the hands of the developers (Jaafar, F., & Butakov, 2020)

2.2.1 PaaS Limitations and Concerns

Data Security. Administrations can use PaaS results to run their applications and services; however, storing data on servers owned by third-party vendors introduces security concerns. For example, organization security alternatives are likely limited if a client has particular hosting limits.

Integrations. On-premise data centers and off-premise clouds may be more difficult to connect to the PaaS offering, limiting the apps and services. It might be difficult to connect legacy IT systems to the cloud if not all of them are cloud-ready.

Vendor lock-in. Decisions about a certain PaaS solution may no longer be relevant due to business and technological needs changes. It may not be possible to transfer to a different

PaaS provider without negatively impacting the company's bottom line if the vendor doesn't provide easy-to-follow migration policies.

Customization of legacy systems. If organizations are using an older version of a program or service, PaaS might not be the ideal choice for the organization. Legacy systems may require certain upgrades and configuration adjustments to work with PaaS. Because of the potential for customization to produce intricate IT systems, PaaS is an expenditure that should be avoided.

Runtime issues. There are circumstances in which PaaS solutions might not be the best option for the languages and frameworks organizations choose to use and the constraints linked with particular applications and services. Depending on the platform, customers can define their dependencies, or it may not be possible.

Operational limitation. As a result of the platform's limitations on the operational capabilities available to end-users, PaaS solutions might not be the best option for cloud operations that involve management automation workflows. By relieving end-users of their responsibility for day-to-day operations, PaaS providers strive to make their services more easily controllable, scalable, and effective.

2.3 IaaS: Infrastructure as a Service

If an organization is looking for cloud computing services that are highly scalable and automated, then need to use infrastructure as a Service (IaaS). Cloud computing services, such as infrastructure as a Service (IaaS), are completely self-service (Copeland & Puca, 2020). Organizations need to be aware of the distinctions between cloud models to make the best decision to find a better model for security issues. A cloud service can fulfill organizations' objectives, whether organizations seek storage options, a simple platform to build custom apps, or complete management over companies' whole infrastructure without maintaining it. The upcoming organization and technology transfer to the cloud, regardless of organization preference.

2.4 Software Failure concerns

Cloud consists of several software that works parallel to ensure its reliability. All the software performs its function and has some responsibility. If any cloud component stops working for any reason, such as partial or whole software failure, it affects the overall cloud computing performance.

Partial software Failure: if any software component stops working, it is a partial software failure. Complete software failure: When complete software fails to respond, it is considered a complete software failure. In the cloud, load balancing has several advantages, including when the volume of traffic increases, servers might get overworked, leading to outages. On the other hand, Cloud load balancing effectively disperses the Load across numerous servers and networks. Load is transferred to another server hub when one of the servers dies or becomes unusable. As a result, the site remains functional even during high traffic periods. Businesses need the correct machines to manage the Load as cloud computing and the sharing of data and information via the Internet grows in popularity. The low cost of cloud balancers makes them an excellent option. It helps them get material out faster, be adaptable, and always be available.

3 Proposed Methodology Framework

This chapter describes the proposed work for this systematic literature review on software failure and security issues. Similarly, this systematic literature review concentrates on the past work from 2019 to 2022 to analyze these studies in detail and check the algorithms, techniques, and methods used

Reasons for selection studies from 2019 to 2022

As the decade changes, cloud computing faces many new challenges tackling security issues and software failure. The researchers has proposed many new security handling algorithms and software failure frameworks. Software failure is a big issue that causes to stop working of the whole organization. When there is some software failure in the organization, there is a chance of data loss that negatively impacts the organization. In our proposed work, we have selected research articles from 2019 and 2022 to explore that issue thoroughly, i.e. software failure and security issues. It will make it easy for researchers to understand the proposed research work on cloud computing software failure and security issues. Moreover, what challenges still needto be tackled in these domains.

Big organizations also select the best reliable software to avoid data theft and failure issues. The latest work in a demonstrated form helps big organizations to find a better solution for theft and failure issues.

3.1 Our contribution

We will deeply analyze the studies and categories in the group to make it better understand the researcher. The group has formed on security issues and their solutions. In the same way, security issues and their solutions.

Our proposed research work will help us understand how the research work has been improved on the issue of cloud software failure and security issues. Moreover, this systematic literature review (SLR) concentrates on the failure of cloud computing software and security issues.

4 Theoretical developed research questions

4.1 Purpose of Review

A large-scale cloud platform uses big data and cloud computing. Data and schemes develop in quantity and complexity, data management, sharing, privacy, software failures, and security issues will occur. Cloud data services allow these issues to be resolved slowly, improving cloud computing speed. The cloud data service may store data in parallel, allowing for data sharing simultaneously. In this scenario, the service provider must maintain data integrity, data privacy, and data confidentiality (Mishra & Janarathanan, 2021), (Rady & Abdelkader, 2019). The storing, retrieving, and sharing of data are the primary causes of concerns regarding cloud computing security. As the load-balancing continues, reliability problems cause the software to malfunction. Therefore, software failure and security concerns are the two most significant problems associated with cloud computing.

Researchers have proposed several frameworks, strategies, and models to solve software vulnerabilities. The study has to examine thoroughly. In the end, a framework and recommendations for existing studies are required.

4.2 Research Questions and Objective

Q1: What are the most typical cloud computing causes of security issues?

Objective: The main goal of the question is to determine the source of cloud computing security issues. Moreover, the evaluation focuses on the researcher's solution to the security issues published between 2019 and 2022.

Q2: what are the main issues of software failure in cloud computing?

Objective: The main goal of this question is to find the main issues in cloud computing that cause the software failure.

Q3: What solutions have been proposed to the cloud computing security issues?

Objective: This question seeks to identify the security challenges in cloud computing and their solution. The proposed work will be evaluated to find a more efficient security solution.

Q3: What solutions have been proposed to tackle the software failure issues?

Objective: Many researchers have proposed frameworks, models, and techniques to overcome software failure issues. So, in this question, they will find the most efficient and convenient solution for software failure.

5 Method and scope of empirical data

This chapter explains several steps to performing a systematic literature review.

5.1 Literature Analysis

Our research methodology includes a complete systematic review following eight-step procedures (Okoli & c, 2015). First, we identify the purpose of our Systematic literature review. Four research questions have been defined and discussed based on the purpose in chapter 4. Security has a different meaning in every field domain. This literature mainly focuses on system security. Also, software failure makes the server or system unavailable, leading to disaster and unavoidable loss costs (Luo & Meng, 2019). In this regard, this research finds some common failure issues and their solution proposed by researchers between 2019 and 2022.

The literature examines the guidelines and planning (Okoli & c, 2015). The second level of examination occurred with research articles—then Organized the informal work manner. Finally, in the end, our proposed study has shared findings from the research articles. The entire process is described in great detail from beginning to end.

An eight-step process developed by (Okoli & c, 2015) for conducting a systematic literature review is used. Moreover, the qualitative approach and methodology are used for analysis.

Step 1. Define the purpose of the analysis

This systematic literature analysis aims to determine the work done on cloud computing software failure and security issues. Moreover, to elicit the most relevant work software failure and security issues.

Step 2: Single Review

By following the (Okoli & c, 2015) procedure, defining the review team and setting the goal for each has to be done in this step. Since a single reviewer is doing this literature review, thus all the synthesis and analysis.

Step 3. Practical screening

Their main plan is to find the research articles from different repositories and organize them in the third step. Other repositories, including google scholar, science direct, and IEEE, allow readers to query requested articles, journals, and books. Moreover, their perception is that all the pieces are available online.

Step 4: literature Search

They ensure all selected repositories, including google scholar, IEEE, and science direct, are explored thoroughly. These steps explain more briefly in this chapter of section 5.2.

Step 5: Extract Data

After querying all the repositories and finding the studies, it has been studied thoroughly to extract the applicable information.

Step 6. Quality appraisal

Quality appraisal rules have to be set for research articles in this step. What articles must be included or what articles must be excluded from succeeding in this step.

Step 7: Synthesize studies:

This step organized the studies based on a qualitative or quantitative approach. A qualitative approach has been applied to this study. This chapter discusses the selected studies' security and software failure issues. The study has been grouped into two sections, e.g., security issues and software failure.

Step 8. Formulation of the results

The result must be formalized after all processes have been completed. The finding and solution discussion chapter has formalized the result. Furthermore, selected studies must be examined further to identify weaknesses and future directions.

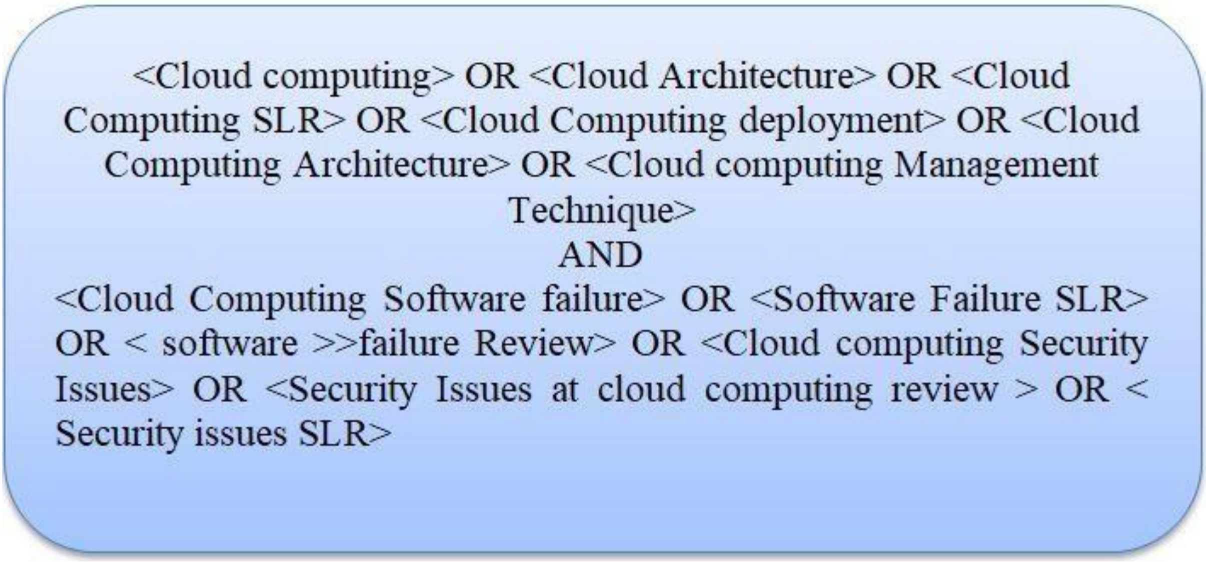
5.2 Literature Search

5.2.1 Practical Screening

In these steps following of the work has been done.

I Search String

We picked this search string because our primary purpose was to look at the suggested storage mechanisms. Figure 1.1 depicts the search string.



<Cloud computing> OR <Cloud Architecture> OR <Cloud Computing SLR> OR <Cloud Computing deployment> OR <Cloud Computing Architecture> OR <Cloud computing Management Technique>

AND

<Cloud Computing Software failure> OR <Software Failure SLR> OR < software >>failure Review> OR <Cloud computing Security Issues> OR <Security Issues at cloud computing review > OR < Security issues SLR>

Figure 1.1 Search String

ii Search Sources

According to the information in Table 5.1, we searched for research papers using Google Scholar, Science Direct, and IEEEXplore, a digital research database maintained by the Institute of Electrical and Electronics Engineers Society. These repositories offer an advanced degree of searching, and you can restrict your query by selecting a certain year, publication, or conference.

	Resources	Hyperlinks
1	IEEEXplore	https://ieeexplore.ieee.org/Xplore/home.jsp
2	Google Scholar	https://scholar.google.com/
3	ScienceDirect	https://www.sciencedirect.com/

Table 5.1 List of selected research resources

Only a few factors (requirements) distinguish high-quality research papers during the selection strategy phase. Table 5.2 shows the rules on which these variables are based. This list of themes and questions was chosen because they were relevant to why people conduct research and what they hope to discover. Choosing the right paper is covered in Table 5.2. All of the documents in stage 2 were written according to these guidelines. Articles were selected for inclusion based on their adherence to the inclusion criteria.

	Inclusion	**Exclusion**
1	Those that at the very least address a single research question in their work	Many academic papers fail to address even the most basic of research questions.
2	We take articles that related to software failures and software security issues	Cloud computing software failure is not mentioned in the papers; only the cloud computing working architecture is discussed. Only the cloud computing issues were explored in the papers, not cloud computing security.
3	Papers published in journals or presented at conferences are included here.	Unpublished research work in conferences and journals.
4	Papers published on security issues and software failures from 2019 to 2022.	Papers that are publishes before 2018
5	All papers are written in the English Language	Articles are not published in the English Language.

Table 5.2: Inclusion and Exclusion Criteria

Table 5.2 shows the inclusion and exclusion criteria of research papers. Five rules have been set to select the paper. Those papers that fulfill the inclusion criteria will be included in this systematic literature review, and others will be excluded. By setting the rules, most relevant research papers will include and exclude. One drawback of the exclusion rule is that only those papers will include that proposed new work to tackle software failure and security issues in cloud computing.

In the first stage, the defined questions will be conducted on the chosen sources. Three sources have been chosen to find the required research work. After completing the stage 1 phase, the move to the 2nd stage; here, all the papers have been downloaded only by reading the title, abstract, or keywords. These three points, title, abstract, and keyword, will glance at the overall paper; if it can fulfill the defined question's requirement, it will be downloaded for further screening.

In the third stage, all the included and excluded rules will be on all the downloaded research papers and chosen to fulfill the included criteria. In the last stage, selected studies were included in the SLR, and a deep study was performed.

Stages	**Applied inclusion and exclusion Criteria**
Stage 1	It was carried out following the research question on the chosen sources
Stage 2	We downloaded all the articles we could locate and read them by scanning the title,abstract, keywords, and anything related to the research issue we were attempting to answer.
Stage 3	Articles were included and excluded following the guidelines.
Stage 4	After carefully considering the available data (SLR), a systematic literature review was selected.

Table 5.3: Paper selection stages according to the criteria of inclusion and exclusion

Table 5.3 shows the applied inclusion and exclusion criteria stages. Research papers were downloaded based on keywords, abstracts, and titles in the first and second stages. In the third stage, all the set rules of inclusion and exclusion are applied, as shown in table 5.2. In this systematic literature review, only those research papers are included that are proposed some solutions to software failure and security issues. Also, those research papers that are published between 2019 to 2022 are only included. By setting the 2019 to 2022 criteria, we aim toinclude the latest research on security and software failure issues.

Moreover, all those papers that do not discuss at least one defined research question have been excluded. This systematic literature review is based on four research questions. So the selection of research papers is also based on the defined research question. Thus, all the selected studies must address at least one research question. Also, the reason for setting the exclusion criteria is to eliminate the irrelevant research papers.

In the first stage from the science direct, google scholar and IEEEXplore papers 97, 400,19 studies. As the figure shows in the 2nd stage, research papers were reduced by doing the scanning. Finally, in the last stage total of 12 papers has selected to perform a systematic literature review.

Repository	Stage 1	Stage 2	Stage 3	Stage 4
Science Direct	97	40	15	3
Google Scholar	400	175	40	5
IEEEXplore	19	17	12	4
Total	516	232	67	12

Table 5.4: Selection of all papers according to stages

5.2.2 Quality Appraisal

Quality refers to the quality of the work, such as whether or not the chosen articles answer the research question. Also, the papers selected came from reputable journals. Moreover, all of the papers are about the years 2019 through 2022. All the criteria have been set in the include and exclude table.

The criteria are set for quality appraisal in the include and exclude table. The selected studies have applied all the rules to ensure quality work.

5.2.3 Formulation of the results

There was much research behind each paper, and comprehension reading had been evaluated. The papers were also written in an approachable tone. Concerns about software and security in cloud computing were addressed in each of the selected articles. Software-related problems were the only focus of some articles, which omitted any discussion of possible remedies. Additionally, there were difficulties securing the facility. Security concerns and software faults are the two main fields of the study analyzed. Security problems are the focus of the next part, divided into further subsections to organize the concerns better. On the other hand, the degree to which information is kept hidden is a major problem for security considerations. Every safety issue developed from the selected research

Similarly, software failure is further divided based on failure issues in the second section. The main issues of software failure are load balancing and less reliable software. These are also big issues of software failure. These issues have been discussed in the finding chapter.

What solution has been proposed to tackle software failure and security issues?

The solution chapter has organized the proposed solution to the software failure and security issues from the selected studies. All the literature has organized the Finding of potential issues and their solutions. The articles are groups on software failure and security issues.

6 Findings : Issues

This chapter will discuss the main issues of software failure and security issues. Also, what problems and effects it has been causing on cloud computing. This chapter is divided into sections. In the initial section, the software failure issues have been discussed in the 2nd section, and security issues in cloud computing have been discussed.

There are four tables given below. The first two tables categorize the selected research paper on software failure and security issues. Similarly, the last two tables organize the chosen research papers on solutions for software failure and security issues. Each table has two columns the second column shows the number of sources and references from Appendix B.

Software Failure issues	No sources and references to Appendix B
Software Reliablity	10
Load Balancing	11,12, 9

Table 6.1 Software Failure and selected Studies

Security issues	No sources and references to Appendix B
Data Integrity	6
Data confidentiality	3,4
Security and Data Privacy	2,5,9

Table 6.2 Security issues and selected studies

Software Failure Solution	No sources and references to Appendix B
Software Reliablity Framework	10
Software Reliablity solution	10
Load Balancing Technique	11, 12

Table 6.3 Software Failure Solutions of selected studies

Security Issues Solution	No sources and references to Appendix B
Multiple encryption techniques	2
Password Encryption	6
Data integrity and confidentiality solution	1
Security Model	7,8

Table 6.4 Software Issues Solutions of selected studies

6.1 Software Failure

Cloud computing has become a versatile and effective method for solving large-scale challenges in the modern world. Many cloud users share computers and virtual resources like services, apps, storage, servers, and networks in an Internet-based computing architecture. These conditions lead to various issues, including long response times, significant power consumption, software failure, load balancing, security issues, and server down.

Now the cloud is used to exchange data across the world. Thus, people can upload the data to the cloud, which can be shared anywhere with a simple link. Now, Their data can be accessed to and from easily. Data can be accessed anywhere and anytime as the cloud has many benefits.

Similarly has some problems such as hardware and software failure, load balancing issues, and reliability issues. The user data can be deleted or destroyed due to software failure, technical issues, or human error because data access multiple users simultaneously. An owner of a cloud service may even conceal data inaccuracies to maintain its reputation or avoid financial loss. Software failure is a critical issue in cloud computing.

6.1.1 Software Reliability issues

In a system failure, the system either fails or shuts down itself. An issue can arise in any node, process, and a network component. As a result, the system experiences a partial failure rather than a complete breakdown (Luo & Meng, 2019). Fault tolerance strategies must be used in high-performance computing even if the systems are more robust and dependable. Because of fault tolerance, even if elements of the system malfunction, the system can still carry out its intended function. A system's fault tolerance (FT) ensures that it can still carry out its intended function when something goes wrong (Luo & Meng, 2019). In other words, FT is all about reliability, performance, and stability. Although some software or hardware may fail, power outages or other unexpected issues may still affect an FT-based system, and it should still meet its needs. For example, Amazon AWS and Ali Cloud advertise 99.9% uptime as a standard feature of their plans (Luo & Meng, 2019).

There is some overlap between classic computer reliability issues like hardware and software in cloud computing regarding integration and development. However, the lines between them are not entirely apparent.

Infrastructure as a Service (IaaS) provides consumers with on-demand access to computing resources in the cloud. Most of the cloud infrastructure's reliability issues stem from hardware failures such as CPUs, memory discs, and network gear (Luo & Meng, 2019). Virtualization, which separates physical assets such as hardware platforms, operating systems, storage devices, and network interfaces, makes IaaS less stable. Applications no longer need to be bound to specific hardware, thanks to the addition of virtualization to the cloud (Luo & Meng, 2019).

Cloud service providers can use a large amount of computing power to manage workloads. Changing virtual machines in the cloud is a challenging issue requiring numerous approaches. When it comes to the reliability of virtualization, virtualization's fundamental feature is virtualization containment. So, even if applications share hosts, failures in other programs would not affect VMs When a VM fails, the hypervisor can isolate it from other VMs to localize the failure. The VMs can be placed in various recovery groups.

High-availability software may be added to aid in the recovery of virtual machines. In addition, because it dictates how most hardware resources are allocated, it could be a single point of failure for a coresident program. Petty utilized a primary and a backup VM hypervisor (Luo & Meng, 2019). Virtualization's stability and how to put and adjust VMs to make them more dependable, available, or fast have been studied by many researchers. The cloud system's performance was improved by disk (Luo & Meng, 2019) revised methods for allocating resources.

The given below table 6.5 shows how much loss companies have faced due to partial or complete software failure. The statistic specifies that amazon bore 45% in 2017 due to faults in storage services (Luo & Meng, 2019).

Date	Cause	Percentage
October 2012	The data servers for Amazon's cloud computing fell, which caused the the shutdown of Reddit, Airbnb, and Flipboard.	30%
February 2017	Amazon AWS S3, fault in storage services	45%
March 2017	The breakdown of Microsoft Cloud Services caused problems for users across the company's platforms, including Outlook, Hotmail, OneDrive, Skype, and the Xbox Live Network.	40%
June 2018	Users could not access the background management interface for Alibaba Cloud, and the photo service function was not working. Strange access was also granted to MCQs, NAS, and other OSS tasks.	The glitch affected more than 40% of China's websites.

Table 6.5: Cloud failure loss statistic (Luo & Meng, 2019).

As shown in Table 6.5, in October 2012, Amazon cloud computing lost 30% of data. Similarly, in February 2017, Amazon AWS S3 lost 45% of its data due to issues with storage services. Also, in march 2017, 40 % of Hotmail, OneDrive, Skype, etc., data were lost due to the breakdown of Microsoft cloud services.

There is no guarantee that data deposited in the cloud will not be tainted or lost owed to hardware, software, or human error. Because when the device fails to work cannot be predicted time with 100% accuracy. It is not only a big issue for cloud users, but also the service providers face the increase in cost and loss of users. Amazon, HotMail, Alibaba, and Cloud services are big services providers; they guarantee their service but still, due to some technical issues, these services break down. Thus, there is no guarantee that the data will not be lost after uploading to cloud computing, as shown in table 6.5.

A cloud owner may cover up data errors to safeguard its reputation or avoid losing money. The integrity of shared cloud data is a pressing issue for many cloud users. Therefore, it is crucial to keep track of it (Fu & Zhang, 2022). There are some common failure issues in cloud computing that are discussed below (Luo & Meng, 2019):

1. **Virtual Machine Failures**

Cloud consists of many virtual machines working parallel to complete a task. The request of any query has to be divided into all the VM. Suppose any virtual machine fails to respond to the query on time. It slows down the system's performance. The service provider claims the high availability has failed here. A virtual machine can be failed due to hypervisor issues and operating system failure. Thus, virtual machine hosts, hypervisors, and operating systems are plagued by problems. Although a VM failure is nearly identical to a hardware failure, the methods for fixing and recovering from a VM failure are vastly different (Luo & Meng, 2019).

2. **Data Inconsistency Failures**

   User data is kept on the server, and cloud application users create intermediary data. Both are the sources of data consistency failures. The low security of the cloud can degrade data consistency (Luo & Meng, 2019).

3. **Redundancy Failures**

   Because they are mapped to virtual computers rather than actual hardware problems, an application's redundant settings are continually changing. It is, therefore, possible for a cloud system to fail. A vital component of a high availability system is monitoring all hardware and redundancy instances reliably and detecting hardware or redundancy failures due to virtualization's impact on conventional redundant setups (such as active/standby). (Luo & Meng, 2019)

6.1.2 Load Balancing

One of the common reasons for software failure is the inefficient load balancing technique. Although many load-balancing techniques have been proposed, service providers still face software failure issues (Zhang & Elgendy,2020). Servers sometimes get the billions and trillions of requests at a time. Which is sometimes difficult to handle and respond to on time? In this scenario, system performance degrades, any component cloud stops responding, and at last, the system crashes. Because according to the SLA, customers get the service up 24/7 hours (Balani & Varol, 2020). In SLA, all the services the service provider provides must be mentioned. Moreover, how long the system can delay the response is noted (Balani & Varol, 2020) (Zhang & Elgendy,2020).

In the cloud, load balancing is distributing the work among multiple servers. Users may obtain content on their computers as rapidly as possible thanks to a software-defined, completely distributed system (Zhang & Elgendy,2020). Workload distribution improves server performance and increases the speed at which users can access server resources by distributing the workload over multiple servers.

The technique of distributing workloads among different computer resources in an environment that uses cloud computing and carefully balancing the network traffic that accesses those resources is referred to as cloud load balancing. The cloud load balancing service also checks to determine if any nodes are under or overloaded and then distributes incoming traffic following this information. In this way, the system can avoid downtime, software failure, excessive power consumption, and other issues caused by overload (Zhang & Elgendy,2020).

Work is distributed among several computing resources to maintain high performance, increase availability, and reduce software failure. With cloud load balancing, clients can distribute their app across numerous clouds worldwide, increasing its resiliency. Load balancers can distribute traffic over multiple servers, even if a single server goes down (Zhang & Elgendy,2020).

6.2 Security Issues

In this section, all the common issues of security have been discussed. Security is a big issue in cloud computing that needs to be tackled. Security concern the growth and downs of cloud computing. Confidentiality, availability, and data privacy are considered the main security issue.

6.2.1 Security and Data Privacy

Personal data can be gathered, stored, relocated, and shared through the cloud computing without putting the privacy of the persons in danger. Customers are often unaware of how their data is stored in the cloud. As cloud computing grows in popularity, protecting user data becomes increasinglycritical (Chen & Jiang, 2020)

In the cloud, the data has to upload by the user, and a user constantly updates the data by adding new information and deleting old data. The user can frequently request the data from the cloud. Here come the problems, the requested data may not be available on the cloud. Cloud management, hardware or software faults, hacker incursions or economic considerations, such as a reduction in the cost of cloud operation, all could causes computing to issues (Chen & Jiang, 2020).

Data security concerns cloud computing when personal information is placed on third-party cloud storage. Stored data can be accessed across distributed and linked cloud resources, regardless of location. For a more secure connection, authentication of these data storage is required (Sharma & Gupta, 2019)

The Internet allows cloud service providers to communicate with one another. It was developed based on TCP/IP, which uses a user's IP address. An IP address is assigned to every Internet-connected machine, virtual or otherwise. Whether legitimate or malicious, anyone can find these IP addresses (Al Nafea & Almaiah, 2021). Moreover, a malicious person can discover which of the victim's physical servers has been compromised to conduct an attack using a malicious virtual machine on that server. If a hacker steals or takes control of a virtual machine, the hacker will access the data of all people who utilize it. Because of this, the hacker has time to copy the files to their PC before the cloud provider realizes the VM is out of control (Al Nafea & Almaiah, 2021). Hackers may be able to find important information from this data.

(Balani & Varol, 2020) stated that there are some of the following security issues in the cloud:

1. **SLA Management:** An agreement between the user and cloud service provider is a service level agreement. It keeps the critical information of the user. If the hacker can access the agreement, it can easily find a significant security threat (Balani & Varol, 2020).
2. **Security Standards:** There are many security standards in the Information Technology Infrastructure Library. Cloud computing is plagued by HTTP Denial of Service and XML-based Denial of Service assaults. It is not difficult for hackers to commit these kinds of felonies. Security is a critical issue for businesses. Cloud users should know security standards to tackle malicious attacks (Balani & Varol, 2020).
3. **Assign Privileges**: It is necessary to double the user authority already assigning the privileges. This authority can take who justifies it. Much of the information made outside the business is risky since outsourced operations go via physical and personnel controls in IT workshop using home software (Balani & Varol, 2020).
4. **Separation of data Sources:** When users request the data on the cloud, the resulting data comes from other data sources. Sometimes it becomes a significant issue to separate the data source. Here comes the problem the resulted data need to encrypt. If it is not handled carefully, the encryption key can be lost. A hacker can encrypt the data using the encrypted key (Balani & Varol, 2020).

5. **Recover**: When customers have problems obtaining data, third parties rarely authorization to be monitored. As a result of this issue, things may become less secure (Balani & Varol, 2020). It is wrong for cloud service providers to be shut down or bought out by large corporations. On the other hand, cloud providers ensure that their data remains accessible.

6.2.2 Data Integrity

As cloud computing has multiplied, consumers have become more concerned about the security and integrity of their data. Cloud platforms' security is increasingly a top consideration when procuring services (Mishra & Janarathanan, 2021).

Various techniques utilizing steganography and cryptography might be employed. As a result, both time and space expenses rise, and the possibility of data loss intensifies. Efforts are continually being made to enhance the existing systems for mistake detection and correction. MD5 and SHA-1 to store passwords are still prevalent in many organizations. A hashing attack can exploit these methods since they are less robust. In this case, the hashed passwords can be cracked using dictionary-based spectral attacks (Mishra & Janarathanan, 2021). A cloud data service provider can store data from many customers. Steganography and cryptography are used together to ensure that complex information is secure.

Cloud storage enables users to get to their data in some ways and keep more of it in the system. But this tends to pose security challenges in cloud storage, and customers worry about how well their data will stay safeguarded. In this example, cloud security has been built, and the user has been handed two secret keys. The secret key is made from a series of random numbers with various steps. The encryption approach is ideal for cloud security because it is based on algebra. Cloud auditing services have been built to prove that the data saved in the cloud is correct. Cloud auditing also has a bad means of security.

6.2.3 Data confidentiality

An outsourced server or an unauthorized user could potentially disclose confidential data, so confidentiality is essential. Data can only be viewed by those granted access by encrypting it (Rady & Abdelkader, 2019). As a result, software, data leakage, and inadequate security issues can be faced. The hardware sharing should be restricted, and nodes should only be accessible to those granted permission. If these and other defenses are implemented, attackers will not determine the destination (Saldamli & Lo'ai, 2021).

Researchers in cloud computing are still attempting to discover answers to the problem of maintaining the confidentiality of user data. Cloud Service Providers (CSPs), also known as Internet Service Providers, compel their customers to cede control over their proprietary business data to an outside service provider. Most data protection protocols currently in use employ cryptography as their primary method. In addition, the cryptographic techniques require additional processing power from the computer, which is especially important when the data is split up among several different CSP servers. Storage as a Service is frequently an excellent option for small and medium-sized organizations that need more storage space but do not have the financial or technical skills necessary to establish and run their storage facility.

7 Finding: Solutions

This chapter will discuss the proposed solution to security issues and software failure. This chapter has two sections; in the first section, all the studies that proposed a solution to security issues have been discussed. In the 2nd section, all the selected studies proposed solutions for software failure have been discussed.

7.1 Security issues solution

Security is a big issue in cloud computing.

7.1.1 Multiple encryption techniques

Encryption is a technique that modifies the data so that only the authentic user can access and read it. It is the most common security technique to secure data on the Internet. A novel multiple encryption techniques were proposed to enhance security (Sharma & Gupta, 2019). It is a multi-level encryption technique. The Encryption method begins with uploading a text file, which the user must do earlier, proceeding to the next steps. After uploading the file, the file will be encrypted using the RSA encryption method. RSA is an algorithm used to encrypt the data on the cloud. Using the RSA technique, encrypt the text file at the first possible level of security. Then in the second phase, the file has to be encrypted using the RSA method again. The third phase uses the AES method to encrypt the text created in the previous two stages. As a result, the file gains a second layer of protection from unauthorized access (AES). In the final phase of encrypting a text file, the cyphertext generated by the previous processes is stored in an encrypted database (Sharma & Gupta, 2019).

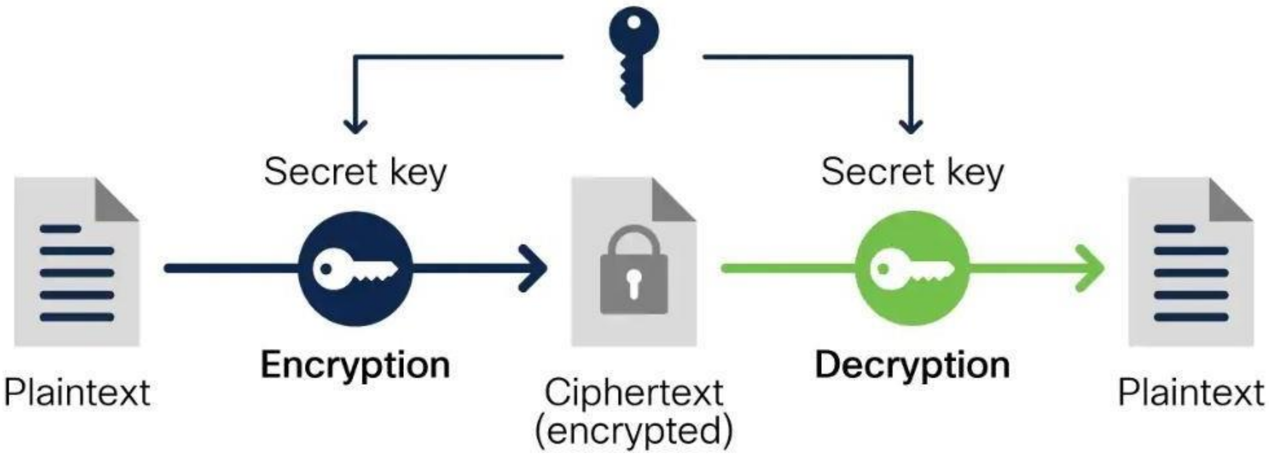


Figure 7.1 Encryption and Decryption

The proposed model (Sharma & Gupta, 2019) provided more secure data storage based on the world's most trustworthy cyphers algorithms, AES and RSA.

7.1.2 Password Encryption

Password is the first step to keeping secure data anywhere. Thus, multiple techniques have been proposed to make unable to break the password. The first step is to create a stronger password than typical to ensure security (Mishra & Janarathanan, 2021). Moreover, many new techniques have been proposed to increase system security through password protection. Similarly, in this regard (Mishra & Janarathanan, 2021) proposed a new password encryption technique. The primary objective is to develop a comprehensive cloud solution by examining the most pressing issues. The goals are to keep an eye on cloud computing and safeguard it from malware threats using the GPU's computing capabilities. Use a method that does not lose any data to reduce the amount of data that needs to be stored—using a single iteration execution to save the most time possible (Mishra & Janarathanan, 2021).

MD5-crypt is a well-known method for encrypting passwords. This method is utilized in Cisco routers, and the Linux distribution supports it. 1502 MD5-compressions are the most critical task of MD5-crypt. The proposed technique has three main types (Mishra & Janarathanan, 2021). In the first step, there are three sections: salt, password, and hash. All the sections are combined and hashed together for initial use. The second step hashes them together using the magic string (1), the password, and the salt. As in the three-step, the password, salt, and the last application's result are all hashed together in a hashing algorithm, starting with n.

MD5-crypt is considered particularly safe since it uses 1500 iterations and mixes the password, salt, and the previous iteration's result in a pseudo-random manner. If the parallelism can be successfully transferred to the different layers of the architecture, then the user experience can be improved significantly. (Mishra & Janarathanan, 2021).

7.1.3 Data integrity and confidentiality solution

Assuring the security of cloud-based data is a significant challenge. In cloud computing, cryptography has been employed to ensure that private information is not compromised. However, there are numerous ways for criminals to evade the security provided by cryptography. They demonstrated multiple levels of data protection by using cryptography and steganography (Mahmood & Huang, 2019). Steganography and cryptography are used together to ensure that sensitive information is protected. First, the secret image is encrypted with the AES encryption algorithm. Second, the encrypted private image is concealed within the cover image using the SVD-DWT hybrid steganography algorithm. Third, a hash method is performed on the hidden file before downloading it from the cloud to ensure it is correct. Simulated images produced by this system have a significant peak signal-to-noise ratio. The approach also reduces the possibility of viewers believing an image contains unreadily apparent information.

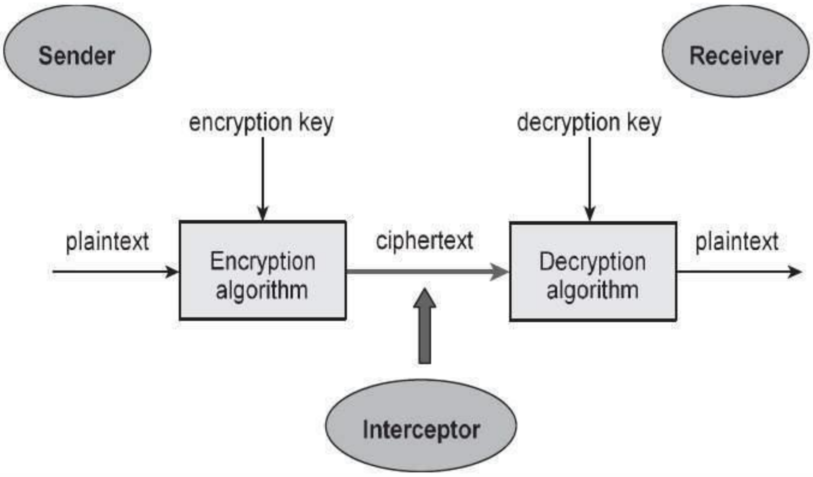


Figure 7.2 Processes of Encryption and Decryption

7.1.4 Security Model

Encryption and decryption can be accomplished using the same technique, which is recommended. They use the AES and RSA cyphers to protect user data, proving it safe and secure (Ahmad & Mahfuz, 2022). The term "cloud computing" refers to obtaining services through the Internet.

They employed a network connection, such as the Internet, to share resources, including servers, storage, applications, and services (Ahmad & Mahfuz, 2022).. It is a relatively recent development in dependable, adaptable, scalable, and stable technology. Computing in the cloud can be brokendown into three primary service models. IaaS stands for "Infrastructure as a Service," whereas PaaS and SaaS refer to "Platform as a Service" and "Software as a Service," respectively (SaaS). Within the IaaS service model framework, the customer can gain remote access to the fundamental IT through the cloud service provider. It makes it easier for the customer to set up these resources whenever required. In this case, the customer does not need to worry about purchasing or operating hardware or data centers because these aspects are handled. IaaS gives its customers the greatest amount of control possible over their cloud computing, more so than any other model; yet, the security of this layer is compromised. One of the primary reasons for this is that access credentials are not set up effectively, enabling anyone to access vital information kept in the cloud. In addition, administrators do not provide their customers with the appropriate log-in details for their cloud services.

PaaS, which stands for "platform as a service," is a form of cloud computing that provides programmers with a foundation and an environment to create web-based applications and services that can be accessed using a web browser. Clients can access the hosted services using their web browsers because they are in the cloud. PaaS providers are there to assist their customers whenever they have a question or concern, from when a customer has an idea until the moment that their application is ready for testing and delivery. However, the operation of the security layer varies from one provider to the next in its entirety. While data is being transferred between personal computers, private information saved on the open web is connected to local networks. Anyone who wants to can read over this information. Therefore, the security of the PaaS layer is in jeopardy.

A method of providing software as a service (SaaS) is one in which software programs are kept in a remote location by a cloud service provider and are made accessible to customers over the Internet whenever those customers need to use those programs. The software as a service (SaaS) business model offers its clientele a variety of advantages, and it is swiftly gaining ground as the method of choice for satisfying requirements relating to IT services. However, many companies continue to lack clarity around the management and security of their data. There is also concern regarding security flaws in the programs themselves and security breaches committed by employees within the company, potentially resulting in the loss of sensitive data. Because of these obstacles, it is difficult for businesses to employ SaaS services hosted on the cloud.

RSA algorithm

RSA stands for Rivest, Shamir, and Adleman. The RSA algorithm is a widely used public-key encryption technique. The data cannot be decrypted if an encryption key is unavailable. The RSA algorithm is a widely used public-key encryption method. Both public and digital signatures can be encrypted using RSA using this method. The most challenging factors have been addressed (Ahmad & Mahfuz, 2022).

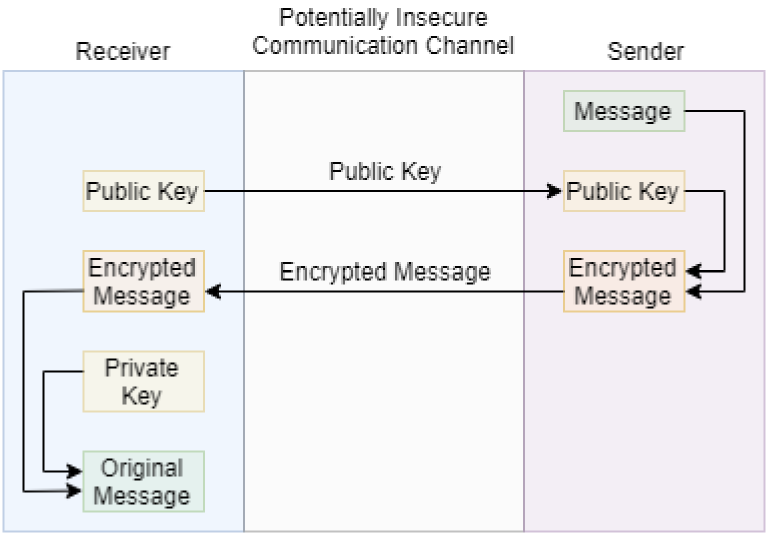


Figure 7.3 Encryption RSA Algorithms

Blowfish

As a replacement for DES and Aging, Schneier created Blowfish because it lacks the drawbacks and limitations of its predecessors. There are 16 rounds in this Feistel cipher, and the chests are long S shapes. There are no moving S squares on the frame in this version of CAST-128. There are no moving S squares on the frame in this version of CAST-128. A 32-bit value is assigned to each line. 256 S and 18P are two of the five primary ranges.

It was stated by (Ahmad & Mahfuz, 2022) that only the authorized user could access the encrypted data. The data must be decrypted if an intruder (an unauthorized user) obtains it, which is challenging to perform without a valid key.

Similarly, (Thabit & Can. (2022) proposed a cloud security technique to enhance security.

They describe a new and successful homomorphic cryptographic approach to two encryption levels. A practical and lightweight cryptographic technique is used for cloud computing's first layer, while multiplicative homomorphic algorithms are used for the second. This method works with symmetric and asymmetric cryptography. Many criteria evaluate the suggested method's effectiveness, counting computational time and recollection usage, key compassion, arithmetical analysis, and entropy alteration analysis using a same histogram. Overall, the proposed technique increases system security.

7.2 Software Failure Solution

This section discusses a detailed discussion of proposed work on software failure.

7.2.1 Reliability Framework

To deliver reliable services, a cloud service provider needs to have a set of core tasks that they can rely on reliability. (Luo & Meng, 2019) discussed a reliability framework to decrease the rate of software failure. The software reliability depends on the number of layers (Luo & Meng, 2019).

1. **Infrastructural layer**

   There are several physical servers and virtual machines in this layer. Random failures and how to fix them need to be considered in this layer and their impact on the number of resources available in an extensive, complex system. If the resources layer is not trustworthy, the application layer will suffer. Because of this, if the infrastructure layer is unreliable, the application service layer above it will be unreliable (Luo & Meng, 2019).

2. **System Management Layer**

   In this layer, the system scalability, capability, and dependability are managed. There are various methods by which the cloud resource manager can control reliability, depending on how resources are utilized randomly (Luo & meng 2019).

3. **Service Management Layer** This layer encompasses cloud applications, desktops, and virtualized resources. Because of the randomness of service requests and the randomness of the underlying resources, the application service and the usage of system resources are similarly unpredictable (the system load is random). The final dynamic performance layer is influenced by system resources as well. Consequently, the application and state-monitoring layers are linked to resource use and system reliability (Luo & meng 2019).

4. **User Layer**
   At this level, customers and service providers agree on SLAs and standards for reliability. Service foundations can offer two levels of service consistency to their customers. Users can request an SLA-backed reliability guarantee in place of the standard reliability guarantee. System suppliers might also offer customers additional guarantees in reliability services (Luo & meng 2019).

7.2.2 Software Reliability solution

Service providers can now employ a novel simulation framework (Luo & Meng, 2019) to implement a reliability scheme and provide cloud users with reliable service. In addition to considering the stability of hardware and virtual machines (VMs), they evaluated their connections to higher-level system services and used multilayer design to assure the system's and services' resilience. Even more importantly, they examined the reliability of large-scale cloud computing systems thoroughly and exhaustively, picking out the fundamental features that may boost system reliability and looking at seven common reasons for system failure, including hardware, software, and platform (Luo & Meng, 2019).

Large-scale cloud computing systems can be predicted using the (Luo & meng, 2019) model. A model that assesses the present level of dependability of the cloud system serves as the foundation for reliability-aware resource scheduling. This technique is based on the reliability concept. Virtual machines are placed and relocated based on the system's current state, determined via this method (Luo & Meng, 2019). CloudSim is used to test the suggested reliability model and reliability-aware algorithm (Luo & Meng, 2019).

7.2.3 Load Balancing Technique

Distribution of the Load by using the shortest path between sender and recipient is a common practice in digital data transmission (Varshney & Gaur,2021). The original server strain is managed using high-performance and reliable surrogate servers. When creating nodes and networks, and NS2 file is created in the initial phase. Then, the client-server architecture was used to write code. There must be as few packet drops as feasible and as many packets delivered as possible when a user requests to transmit a message from source to destination. When comparing findings by (Varshney & Gaur 2021), the throughput, packet drop, delay, and packet delivery ratio improved.

Because of the many advantages of cloud computing, many organizations have switched to it (Varshney & Gaur,2021). Combining servers and reducing infrastructure expenses are just some of the advantages of virtualization. It is also possible to move a virtual machine from one server to another in nearly no time (Awatif & Amina, 2019).

However, intelligent and self-managing management approaches are required to evenly distribute the workload among datacenters' millions of virtual machines (Awatif & Amina, 2019). Most of what ACO is built on is how ants navigate from their nests to food sources (Awatif & Amina, 2019). Balance of workload, response time, and processing time are the three main objectives of the algorithm under consideration. This algorithm's pheromone formula has been altered so it may be used in Cloud computing. According to the Ain CloudAnalyst simulations, the suggested algorithm outperforms the existing ones (Awatif & Amina, 2019). Mobile edge computing is a new approach to cloud computing. That solves the problem of limited resources for handheld and mobile devices. Using cloud computing on mobile devices can assist in compensating for the devices' limited storage space. A "computation offloading" technique uses a central cloud to handle computationally expensive jobs. Overloaded sBSs may not be able to complete computing tasks within the acceptable latency threshold because they must spend too much time communicating and processing data. In the meantime, inadequate attention has been paid to the security vulnerabilities that arise from data offloading. Devices are additionally protected using an advanced encryption standard cryptographic method that uses encryption and decryption solutions derived from electrocardiogram signals.

Load-balancing algorithms are proposed (Zhang & Elgendy,2020) to re-distribute MDU tasks among SBS, in which users are assigned to the best-available SBS based on variables such as its geographic location and current user count, as well as the number of CPU cycles per MUD task and the maximum uplink data rate. Encryption and decryption keys based on ECG signals are used in conjunction with an AES cryptographic technique to add a new layer of security. Multi-user cloud computing systems require a combination of load balancing and compute offloading to overcome resource constraints (i.e., having reduced overhead). A safe balancing and computation offloading technique is devised with no additional effort to find the best response swiftly. An energy savings of 68% to 72% is possible with or without enhanced security when using the proposed technique (Zhang & Elgendy,2020).

8 Analysis and Discussion

Most of the time, security literature focuses on only one of the affected security sectors. Most of the study articles did not delve into smaller research areas that might be considered a potential danger to the future of cloud computing. Security of the physical system is another example. The physical system is not usually seen as a considerable security problem.

This risk is often neglected even if it is written about in a small literature section. Since a malicious or uneducated user might be a concern in all parts of an organization, it is logical that they are not considered a primary threat in the literature that concentrates on a specific risk. However, only a tiny part of the literature tried to isolate the various security problems and solutions for each service type.

As service models are one of the most significant for cloud computing. The same can be stated about the numerous deployment types, but the fact that they are not discussed is as significant a problem as the service models. There are more evident differences between the types of deployment. Similarly, (Sharma & Gupta, 2019) proposed a multi-level encryption technique to increase security. They used two encryption algorithms, AES and RSA. Multilayers encrypt the data; RSA has applied twice in the first layer, then AES. This way, data is encrypted in a format only the authentic user can access.

The public cloud is more likely to have malicious users because the organization that administers the cloud cannot track who uses it. Unlike a private cloud, where the cloud provider has more control over who can access the data, this is a public cloud. The public cloud is vulnerable to attacks and theft of data. Moreover, several causes can explain why there is not much published about these sub-areas. First, research has been done in these areas but may not have been published as a cloud computing security concern. For example, some works are published under cloud computing but not security or cloud computing security (Zhang & Elgendy,2020).

Security issues concern the overall impact on business growth and success. Besides security issues, software failure is also a big issue in cloud computing. Several research articles have been published to tackle the issue of software failure, including load balancing techniques, fault tolerance models, and reliable software systems. Most of the research stated that Software failure occurs when software is not reliable. But that is not the only issue; other factors also play a vital role, such as planned reboot, unplanned reboot, software update, lack of resources, and immature technology.

Some of the security threats organization faces

When companies shift their project to the cloud, they lose control and insight over their assets and processes. Cloud service providers take over some of the policies and infrastructure as the companies shift to the cloud. Whether cloud service models are employed, agencies must adapt how they monitor and record security. On-premises IT network-based monitoring and logging is not an option for organizations that need to monitor and analyze applications, services, data, and people (Sharma & Gupta, 2019). Cloud service providers make it quite simple to launch new services. Employees of a company can take advantage of the CSP's on-demand self-service provisioning to access more services. Self-service provisioning refers to utilizing software that the organization's IT department does not provide.

Two types of Paas and Saas(software as a service) are more prone to be misused because these are less expensive and easy to implement. A firm faces dangers when IT services are put up or used without knowledge. Unapproved cloud services could result in more malware attacks or data theft because an organization cannot defend resources. A corporation's ability to monitor and regulate its network and data becomes more difficult when it uses cloud services that the company does not authorize. Application programming interfaces (APIs) provided by cloud service providers (CSPs) help clients control and interact with cloud services (also known as the management plane). An organization's assets and users are monitored and managed through these APIs. As with any other software API, these too may be vulnerable to the same problems that plague other kinds of APIs. Because they are available via the Internet, CSP APIs are distinct from on-premises computer management APIs. As a result, they can be put to more varied and creative uses.

Treacherous individuals can exploit management APIs. The cloud assets of a company can be taken over if these flaws are discovered and exploited. The attackers can then use the organization's resources to launch additional attacks against other cloud service provider clients. Software flaws in CSP infrastructure, platforms, or multi-tenancy applications can make it impossible for tenants to be kept apart. Using a resource from another organization, an attacker could gain access to the assets or data of a different user or organization (Luo & Meng, 2019). If the separation measures fail, data leakage is more likely because of the increased attack surface provided by multi-tenancy. Bypassing logical isolation controls or attacking the CSP's management API, an attacker can exploit the applications, hypervisor, or hardware weaknesses of the CSP.

Customers may not know where their data is stored in the cloud and may not be able to verify that their data has been safely deleted when they delete it. This threat is troublesome because the CSP's infrastructure has various storage devices. This type of setup is referred to as a multi-tenancy one. It is also possible that the process of deleting may vary from one service provider to another. In some cases, organizations may not be able to be certain that their data has been deleted completely and that any traces of it are no longer accessible by hackers. This danger increases in proportion to the amount of CSP services a given organization utilizes.

This systematic literature review has set rules about which research papers can be included and which ones cannot. This systematic literature review did not include research papers that did not meet the criteria. Some papers were not fully published, but the abstracts show a robust security model. Similarly, some research papers only talked about software failure problems but did not say how to fix them. Because of the second rule of exclusion, we cannot add what they say in their discussion to our systematic literature review. We have answered all four questions in the finding and solution chapter. In the finding chapter, we have covered all issues regarding the security concern and software failure issues in cloud computing. The solution chapter shows the result of the proposed solution on security and software failure concerns.

9 Concluding discussion/ remarks

This literature study used cloud computing security methodically to determine the significant security problems with this technology. Criteria picked the first 516 articles to decide what literature to include in the review. These papers were then looked at more depth, and 12 were deemed relevant to the study topics. Using these 12 publications, we determined the most critical cloud computing security concerns, solutions, and areas that need more research.

Q1: What are the most typical cloud computing causes of security issues?
We have covered the primary causes of security problems, such as data integrity and confidentiality, in my response to this question. It is covered in the chapter finding: issues.

Q2: what are the main issues of software failure in cloud computing?
The primary causes of security problems, such as data integrity and confidentiality, are covered in the answer to this question. We have discussed in the chapter finding: issues.

Q3: What solutions have been proposed to the cloud computing security issues?
We found research that suggested some few solutions to the security problems with cloud computing in the response to this question. It is discussed in the chapter finding: solution.

Q4: What solutions have been proposed to tackle the software failure issues?
In the finding: solution chapter, we referenced a number of studies that addressed the main reasons of software failure, such as load balancing and software reliability, in response to this question.

9.1 Limitation of the review

A wide range of sources was an objective of the review, although it is impossible to include all of the available literature. As a result, some standards were devised to select appropriate literature. There is a risk that some important works were overlooked because of these criteria. In addition, just three databases were tapped into for the study. The three selected sources including google scholar, IEEEXplore, and Science Direct are very good repository and the most trusted in the regards of cloud computing software failures and security issues research articles. Even though they believe this is sufficient, some significant material may have been overlooked. As a result, a concise list of existing security issues and potential remedies was created.

9.2 Outcome

As a theoretical starting point for future research, this review demonstrates today's most pressing security issues and some potential answers to those concerns. This review's hypothetical answers need to be tested in real-world scenarios, so more study is needed in this area. In addition, further research is required to discover how cloud computing customers and cloud service providers view security. Finally, future studies should investigate how various deployment strategies and service models affect a system's security.

References

Ahmad, S., Mehfuz, S., & Beg, J. (2022). Assess potential security threats and introduce a novel data security model in a cloud environment. *Materials Today: Proceedings*.

Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: A literature review. In *2021 International Conference on Information Technology (ICIT)* (pp. 779-786). IEEE.

Ali, B., Gregory, M. A., & Li, S. (2021). Multi-access edge computing architecture, data security and privacy: A review. *IEEE Access*, *9*, 18706-18721.

Ali, A. Q., Sultan, A. B. M., Abd Ghani, A. A., & Zulzalil, H. (2019). A systematic mapping study on the customization solutions of software as a service applications. *IEEE Access*, *7*, 88196-88217.

Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi,
H. A. (2021). Cloud computing in the construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.

Chen, F., Li, Z., Jiang, C., & Li, J. (2020). Verifiable Cloud Data Access: Design, Analysis, and Implementation. *IEEE Systems Journal*.

Fu, A., Yu, S., Zhang, Y., Wang, H., & Huang, C. (2022). NPP: a new privacy-aware public auditingscheme for cloud data sharing with group users. *IEEE Transactions on Big Data*.

Luo, L., Meng, S., Qiu, X., & Dai, Y. (2019). Improving failure tolerance in large-scale cloud computing systems. *IEEE Transactions on Reliability*, *68*(2), 620-632.

Luo, L., Meng, S., Qiu, X., & Dai, Y. (2019). Improving failure tolerance in large-scale cloud computing systems. *IEEE Transactions on Reliability*, *68*(2), 620-632.

Lo'ai, A. T., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobilecloud systems. *Journal of King Saud University-Computer and Information Sciences*, *33*(7), 810-819. Rady, M., Abdelkader, T., & Ismail, R. (2019). Integrity and confidentiality in cloud outsourceddata. *Ain Shams Engineering Journal*, *10*(2), 275-285.

Isharufe, W., Jaafar, F., & Butakov, S. (2020, June). Study of Security Issues in Platform-as-a-Service (PaaS) Cloud Model. In *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)* (pp. 1-6). IEEE.

Mahmood, G. S., Huang, D. J., & Jaleel, B. A. (2019). Achieving an Effective, Confidentiality andIntegrity of Data in Cloud Computing. *Int. J. Netw. Secur.*, *21*(2), 326-332.

Mishra, J. K., & Janarthanan, M. (2021). GPU-based security of password hashing in cloud computing. *Materials Today: Proceedings*.

Odun-Ayo, I., Ananya, M., Agono, F., & Goddy-Worlu, R. (2018, July). Cloud computing architecture: A critical analysis. In *2018 18th international conference on computational science and applications (ICCSA)* (pp. 1-7). IEEE.

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. Communications of the Association for Information Systems, 37(1), 43

Sharma, Y., Gupta, H., & Khatri, S. K. (2019, February). A security model for the enhancement of data privacy in cloud computing. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 898-902). IEEE.

Soh, J., Copeland, M., Puca, A., & Harris, M. (2020). Overview of Azure Infrastructure as a Service (IaaS) Services. In *Microsoft Azure* (pp. 21-41). Apress, Berkeley, CA.

Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. *International Journal of Intelligent Networks*.

Varshney, P., Gaur, S., & Pal, S. (2021, January). A novel approach of Load Balancing in Content Delivery Networks by optimizing the surrogate server. In *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 790-795). IEEE.

Zhang, W. Z., Elgendy, I. A., Hammad, M., Iliyasu, A. M., Du, X., Guizani, M., & Abd El-Latif, A. A. (2020). Secure and optimized Load balancing for multitier IoT and edge-cloud computing systems. *IEEE Internet of Things Journal*, *8*(10), 8119-8132

Appendix A

This study systematically examined cloud computing security issues and software failure studies to find its primary security vulnerabilities and failure cause. The first 67 articles were picked using criteria. 12 of these papers were connected to the research issues after further review. This evaluation examined 12 papers to identify cloud computing security issues, treatments, and research gaps.

A: Paper Number
B: Research Title
C: Publication Year
D: Publication Type
E: Credible Author?
F: Research Question relevant
a: Question 1
b: Question 2
c: Question 3
G: Include in review?

A	B	C	D	E	F	G
1	Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing	2019	Journal	Yes	Yes	Yes
2	A Security Model for the Enhancement of Data Privacy in Cloud Computing	2019	Conference	yes	yes	Yes
3	Integrity and Confidentiality in Cloud Outsourced Data	2019	Journal	Yes	Yes	Yes
4	Reconsidering Big Data Security and Privacy in Cloud and Mobile Cloud Systems	2021	Journal	Yes	Yes	Yes
5	Verifiable Cloud Data Access: Design, Analysis and Implementation	2020	Journal	Yes	Yes	Yes
6	GPU-based security of password hashing in cloud computing	2021	Journal	Yes	Yes	Yes
7	Assessment of potential security threats and	2022	Conference	Yes	Yes	Yes

	introducing novel data the security model in the cloud environment					
8	A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing	2022	Journal	Yes	Yes	Yes
9	Cloud Computing Security Challenges and Threats	2020	Journal	Yes	Yes	Yes
10	Improving failure tolerance in large-scale cloud computing systems	2019	Journal	Yes	Yes	Yes
11	Secure and optimized Load balancing for multitier IoT and edge-cloud computing systems	2020	Journal	Yes	Yes	Yes
12	A novel load Balancing approach in Content Delivery Networks by optimizing the surrogate server.	2021	Conference	Yes	Yes	Yes

Appendix B

The sources listed in appendix A are all included in this appendix. This section does not include other sources outside the 12 listed in appendix A. It is also available in the reference section. In the same way as appendix A, the sources are listed in the same order.

1. Mahmood, G. S., Huang, D. J., & Jaleel, B. A. (2019). Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing. *Int. J. Netw. Secur.*, *21*(2), 326-332.

2. Sharma, Y., Gupta, H., & Khatri, S. K. (2019, February). A security model for the enhancement of data privacy in cloud computing. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 898-902). IEEE.

3. Rady, M., Abdelkader, T., & Ismail, R. (2019). Integrity and confidentiality in cloud outsourced data. *Ain Shams Engineering Journal*, *10*(2), 275-285.

4. Lo'ai, A. T., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. *Journal of King Saud University-Computer and Information Sciences*, *33*(7), 810-819.

5. Chen, F., Li, Z., Jiang, C., & Li, J. (2020). Verifiable Cloud Data Access: Design, Analysis, andImplementation. *IEEE Systems Journal*.

6. Mishra, J. K., & Janarthanan, M. (2021). GPU-based security of password hashing in cloud computing. *Materials Today: Proceedings*.

7. Ahmad, S., Mehfuz, S., & Beg, J. (2022). Assessment on potential security threats and introducing novel data security model in cloud environment. *Materials Today: Proceedings*.

8. Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. *International Journal of Intelligent Networks*.

9. Balani, Z., & Varol, H. (2020, June). Cloud Computing Security Challenges and Threats. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-4). IEEE.Luo, L., Meng, S., Qiu, X., & Dai, Y. (2019). Improving failure tolerance in large-scale cloud computing systems. *IEEE Transactions on Reliability*, *68*(2), 620-632.

10. Zhang, W. Z., Elgendy, I. A., Hammad, M., Iliyasu, A. M., Du, X., Guizani, M., & Abd El-Latif,

    A. A. (2020). Secure and optimized Load balancing for multitier IoT and edge-cloud computingsystems. *IEEE Internet of Things Journal*, *8*(10), 8119-8132.

11. Varshney, P., Gaur, S., & Pal, S. (2021, January). A novel approach of Load Balancing in Content Delivery Networks by optimizing the surrogate server. In *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 790-795). IEEE.